UCE Techniques de Tests
TP 3

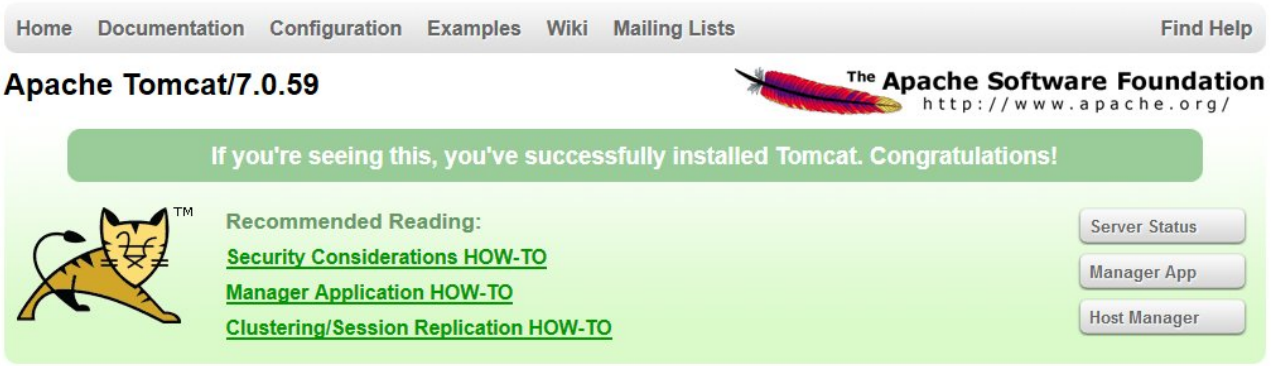
UE Génie Logiciel Avancé
M1 ILSEN

TP 3

- Objectif
  - Effectuer des tests de sécurité d'une application Web
  - Tester l'application de formation WebGoat qui est
    - un projet de l'Open Web Application Security Project
    - une plate-forme de formation permettant à un utilisateur d'apprendre à exploiter les vulnérabilités les plus courantes sur une application Web
- Déroulement
  - Installez l'application WebGoat
  - Pour chacune des « leçons » sélectionnées
    - Exploitez la vulnérabilité et indiquez le code source en cause
    - Qualifiez en rapport avec le cours

TP 3

- Installez OWASP WebGoat
  - Installez Tomcat 7.0
    - Téléchargez et décompressez apache-tomcat-7.0.59.zip
    - Donnez les droits d'exécution aux scripts shell de ./bin
    - Lancez le serveur (voir RUNNING.txt)
    - Vérifiez son fonctionnement : http://localhost:8080/
    - Arrêtez le serveur tomcat



TP 3

- Installez OWASP WebGoat
  - Installez WebGoat-5.4
    - Téléchargez WebGoat-5.4.war dans ./webapps
    - Ajoutez les lignes ci-dessous au fichier ./conf/tomcat-users.xml

```
<role rolename="webgoat_basic"/>
<role rolename="webgoat_admin"/>
<role rolename="webgoat_user"/>
<role rolename="tomcat"/>
<user password="webgoat" roles="webgoat_admin" username="webgoat"/>
<user password="basic" roles="webgoat_user,webgoat_basic" username="basic"/>
<user password="tomcat" roles="tomcat" username="tomcat"/>
<user password="guest" roles="webgoat_user" username="guest"/>
```

    - Redémarrez le serveur tomcat
    - Connectez vous à http://localhost:8080/WebGoat-5.4/attack en guest

TP 3

- Rendu pour chaque leçon
  - Indiquez les éléments utilisés pour atteindre le but
    - Uniquement l'énoncé (Lesson Plan)
    - Le ou les indices (Hints)
    - Cookies, Paramètres ou Code source Java
    - La solution de la leçon
  - Qualifiez les différents tests en lien avec le cours
    - Objectif(s) de sécurité et menace(s) liées à l'exploitation de la vulnérabilité telle que proposée dans la leçon
    - Top 10 2013 et 2017 des Risques de Sécurité des Applications OWSAP
  - Indiquer le ou lignes de code java à l'origine de la vulnérabilité
    - Si le code est disponible

TP 3

- Les 9 leçons WebGoat à traiter
  - Access Control Flaws > Using an Access Control Matrix
  - Code Quality >Discover Clues in the HTML
  - Injection Flaws > String SQL Injection
  - Injection Flaws > Database Backdoors > Stage 1
  - Improper Error Handling > Fail Open Authentication Scheme
  - Parameter Tampering > Bypass HTML Field Restrictions
  - Cross-Site Scripting (XSS) > Cross Site Request Forgery (CSRF)
  - Session Management Flaws > Spoof an Authentication Cookie
  - Malicious Execution > Malicious File Execution